WHAT IS CLAIMED IS:

1. A method of secure file transfer between a first client and a second client each communicably connected to a secure file transfer server implementing a process-based security system, comprising the steps of:

authenticating a first client;

checking a first client resource access table for permission to store data;

receiving data from said first client;

storing said received data in secure file transfer storage;

authenticating a second client;

receiving a request from said second client for access to said stored received data;

checking a second client resource access table for permission to access said stored received data;

providing access to the second client where the second client resource access table indicates access permission; and

denying access to the second client where the second client resource access table does not indicate access permission.

2. The method of claim 1, wherein said first client and said second client are each communicably connected to a secure file transfer server by a network.

3. The method of claim 1, wherein said first client comprises a first process.

4. The method of claim 3, wherein said step of checking the first client resource access table includes checking permission for said first process to store data.

5. The method of claim 1, wherein said second client comprises a second process.

6. The method of claim 5, wherein said step of checking the second client resource access table includes checking for permission for said second process to access stored data.

7. The method of claim 1, wherein said received data is stored in a directory.

8. The method of claim 7, wherein said step of checking the second client resource access table includes checking for permission for said second client to access stored data stored in said directory.

9. The method of claim 7, wherein said step of checking the first client resource access table includes checking for permission for said first client to store data in said directory.

10. The method of claim 1, wherein said first client and said second client are each communicably connected to said secure file transfer server using a secure transfer protocol.

11. The method of claim 10, wherein said secure transfer protocol is a secure socket layer transfer protocol.

12. A system for secure file transfer between a first client and a second client, each communicably connected to a secure file transfer server with a process-based security system, comprising:

a secure file transfer server processor communicably connected to at least a first client and a second client;

secure file transfer server storage connected to said secure file transfer server processor having a first client resource access table and a second client resource access table stored thereon;

wherein said secure file transfer server processor authenticates said first client and checks the first client resource access table for permission to write files;

said secure file transfer server processor receives data from said first client and stores said received data in said secure file transfer server storage;

said secure file transfer server processor authenticates said second client and checks the second client resource access table for permission to access files; and

allowing said second client to access said file.

13. The system of claim 12, wherein said first client and said second client are each communicably connected to a secure file transfer server processor by a network.

14. The method of claim 12, wherein said first client comprises a first process.

15. The method of claim 14, wherein said secure file transfer server processor checks the first client resource access table to determine permission for said first process to store data.

16. The system of claim 12, wherein said second client comprises a second process.

17. The system of claim 16, wherein said secure file transfer server processor checks the second client resource access table to determine permission for said second process to access stored data.

18. The system of claim 12, wherein said received data is stored in a directory.

19. The system of claim 18, wherein secure file transfer server processor checks the second client resource access table to determine if there is permission for said second client to access stored data stored in said directory.

20. The system of claim 18, wherein said secure file transfer server processor checks the first client resource access table to determine if there is permission for said first client to store data in said directory.

21. The system of claim 12, wherein said first client and said second client are each communicably connected to said secure file transfer server using a secure transfer protocol.

22. The system of claim 21, wherein said secure transfer protocol is a secure socket layer transfer protocol.